

REMARKS

I. Summary of Office Action

Claims 1-7 are pending in the application.

The Examiner indicated that the drawings submitted with applicants' July 19, 2004 Reply to Office Action should be resubmitted on sheets that are each labeled "Replacement Sheet" in the header.

The Examiner acknowledged receipt of applicants' Supplemental Information Disclosure Statement mailed on October 27, 2004.

The Examiner rejected claims 1-7 under 35 U.S.C. § 102(e) as being anticipated by Win et al. U.S. Patent No. 6,182,142 (hereinafter, "Win").

II. Summary of Applicants' Reply

Applicants submit herewith the drawings previously filed on July 19, 2004 except that the drawings are now on sheets that are each labeled "Replacement Sheet" in the header.

The Examiner's rejection of claims 1-7 under 35 U.S.C. § 102(e) is respectfully traversed.

Reconsideration of this application is respectfully requested.

III. Submission of Drawings

As required by the Examiner, applicants submit herewith replacement sheets of the drawings that were previously filed with applicants' July 19, 2004 Reply to Office Action. In accordance with 37 C.F.R. § 1.121, each of these sheets are labeled "Replacement Sheet" in the header.

IV. The Rejection Under 35 U.S.C. § 102(e)

The Examiner rejected claims 1-7 under 35 U.S.C. § 102(e) as being anticipated by Win. The Examiner's rejection is respectfully traversed.

Applicants' independent claim 1 relates to a method for identifying a component of an electronic system that accessed a resource of the electronic system using an electronic security value unit. As amended, independent claim 1 includes the following features (emphasis added):

- (a) creating an electronic security value unit;
- (b) distributing said electronic security value unit to said component;
- (c) creating a first association between said component and said electronic security value unit;
- (d) providing said electronic security value unit from said component to a resource manager in exchange for access to said resource;
- (e) creating a second association between said electronic security value unit and said access to said resource;
- (f) analyzing said second association to determine that said electronic security value unit was used to access said resource; and
- (g) analyzing said first association to determine that said component accessed said resource.

Win, on the other hand, discusses a method for controlling access by a user to resources stored on one or more protected Web servers using a cookie (token) that identifies one or more roles of the user (*see, e.g.*, Win, columns 5-8). More particularly, system administrators in Win may restrict a user's access to resources by assigning one or more roles to the user defining the user's information needs and assigning one or more roles to each resource. The role(s) assigned to a user in Win may reflect, for example, the user's relationship to an organization (such as employee, customer, or distributor), the user's department within the organization (such as the sales department or engineering department), or other functions of the user. Following an initial login by the user, the user's browser is provided a cookie that includes encrypted information identifying the roles that have been assigned to the user. When the user desires access to a resource of a protected Web server, the user's browser sends a copy of the cookie along with an open URL request to the Web server. The user is then granted access to the resource only if it is determined from the decrypted information that the user has at least one role needed to access the resource. Thus, by assigning (or deleting) a role to the user, access can be added (or deleted) for all resources with that role. Similarly, by adding (or removing) a role to a resource, access can be given (or taken away) from all users with that role.

In contrast to applicants' independent claim 1, Win does not disclose either "creating a second association between [an] electronic security value unit and [an] access to [a] resource" or "analyzing [the] second association to determine that [the] electronic security value unit was

used to access [the] resource” (claim 1). As recited in Win at column 6, line 65 to column 7, line 5:

When the user selects a resource, the browser sends an open URL request and cookie to a Protected Web Server. A Protected Web Server is a web server with resources protected by the Runtime Module. The Runtime Module decrypts information in the cookie and uses it to verify that the user is authorized to access the resource. The cookie is also used by the resource to return information that is customized based on the user’s name and roles.

However, even assuming that a cookie is the same thing as an electronic security value unit (which applicants submit it is not), nowhere in Win is it disclosed that any association be created between the cookie and the access that was obtained using the cookie (as required by claim 1). Rather, a cookie as disclosed in Win is simply used to indicate all of the resources that the user is authorized access to (based on the user’s information needs, as determined by the user’s assigned role(s)). Similarly, Win does not disclose analyzing an association (or anything else) to determine that a particular cookie was used to access a resource.

In rejecting the claims, the Examiner has stated that:

The cookie/token (electronic security value unit) also includes a second association with the resources wherein by analyzing the second association determines a list of customized information that includes the user’s name and role in regards to accessing the requested resources (col. 3, lines 21-31 and col. 7, lines 1-5).

Office Action, page 4, lines 6-10. Applicants presume that the Examiner, in stating that Win’s cookie “includes” a second association with resources, is referring to the fact that the role(s) identified by a user’s cookie determine whether the user is authorized to access particular resources. Contrary to the Examiner’s suggestion, it is respectfully submitted that this connection between a user’s cookie in Win and the resources that the user is authorized to access is not the same as applicants’ claimed second association that is created between an electronic security value unit and an actual access to a resource that has been obtained by a component. Nowhere does Win disclose that upon accessing a resource there is any association created between that access and the cookie that identified permission for that access. Rather, the cookie used in Win is simply used to determine to which resource(s) the user can gain access to. Therefore, Win does not show or suggest a method for identifying a component that accessed a resource including, among other things, “creating a second association between said electronic security value unit and said access to said resource” as claimed in independent claim 1.

Moreover, applicants respectfully submit that Win's disclosure of using a cookie to "return information that is customized based on the user's names and roles" (Win, column 7, lines 1-5), which was referred to by the Examiner, does not in any manner show or suggest "analyzing [a] second association" following an access to determine that a particular cookie was used to obtain the access, as required by applicants' claim 1. Even assuming arguendo that a second association is disclosed in Win (which applicants submit it is not), nowhere in Win is there disclosed the ability (or desire) to analyze such an association to determine that a particular cookie was used for a particular access, for example, when the user has used multiple cookies over time as individual cookies have timed out. Cookies in Win simply indicate the resource(s) a user is authorized to access. However, no mechanism is disclosed in Win to determine, after the fact, that a particular cookie was used for a particular access. Moreover, applicants respectfully submit that neither column 3, lines 21-31 of Win, which was referred to by the Examiner, nor any other portion of Win, discloses analyzing an association to determine that a particular cookie was used to obtain a particular access to a resource. Therefore, Win does not show or suggest a method for identifying a component that accessed a resource including, among other things, "analyzing said second association to determine that said electronic security value unit was used to access said resource" as claimed in independent claim 1.

For at least the foregoing reasons, applicants respectfully submit that independent claim 1 is allowable over Win. Since independent claim 1 is allowable Win, claims 2-7 depending therefrom are also allowable over Win. Therefore, applicants respectfully request that the rejection of claim 1, and claims 2-7 which depend from claim 1, be withdrawn by the Examiner.

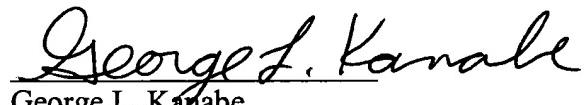
V. Conclusion

For at least the reasons set forth above, applicants respectfully submit that this application, as amended, is in condition for allowance. Reconsideration and prompt allowance of the application are respectfully requested.

Respectfully submitted,

WILMER CUTLER PICKERING
HALE AND DORR LLP

Date: June 13, 2005


George L. Kanabe
Registration No. 51,858
Agent for Applicants

Wilmer Cutler Pickering Hale and Dorr LLP
399 Park Avenue
New York, NY 10022
Tel. 212-230-8800
Fax. 212-230-8888
Customer No. 28089